PRE-APPEAL BRIEF REQUEST FOR REVIEW

REMARKS

Applicants previously submitted that neither Council, Ji et al., nor Hardy et al. disclose or fairly suggest **forwarding or re-routing** from the **recipient computer** to a **screening server**. Applicants' representative and the Examiner agreed that the reference to Ji et al. was relied upon in all the rejections for the virus-scanning limitations. Applicants' representative and the Examiner further agreed that Ji et al. teaches scanning **at the client node** (recipient computer). See, e.g., the abstract and figures 11a-11c and the related text in columns 15-16.

Applicants' representative discussed the following with respect to the claim limitations:

- Claim 1 includes "wherein **said recipient computer further comprises software instructions for forwarding all email messages received to the email screening server;**"
- Claim 6 includes "**software on a recipient computer rerouting email received by the email recipient computer to the email screening server over the network;**" and
- Claim 10 includes "**a recipient computer re-routing received email from the recipient computer to a screening server over a network.**"

Applicants' representative then submitted that the prior art failed to teach or fairly suggest forwarding or re-routing of e-mail messages received at a recipient computer to a screening server. The prior art teaches scanning at ISP-level (e.g., BrightMail) or at the firewall/gateway server prior to delivery to a recipient computer or scanning at a recipient computer (e.g., Norton anti-virus). The ordinary path of e-mail delivery is followed. In the present invention, the path is extended by having **all the e-mail sent back out to a screening server** before any ultimate delivery back to the recipient. As such, a user is not limited to what ISP they use and is not required to make updates to any local virus screening software.

In response, the Examiner and Applicants' representative agreed that the Ji et al. patent failed to teach or fairly suggest forwarding or re-routing of e-mail messages received at a recipient computer to a screening server such that the rejections in the Office Action mailed

October 7, 2004 failed to make a *prima facie* case of obviousness and that further search and consideration by the Examiner was required.

The most recent rejection, mailed May 17, 2005, apparently substitutes the published application of Hypponen et al. for the Ji et al. reference, but suffers from essentially the same problems previously discussed with the Examiner regarding Ji et al., as submitted below.

Claim Rejections - 35 USC 103

Claim 1 was rejected under 35 USC 103 as being obvious over Council in view of Hypponen et al.

Claims 2-15 were rejected under 35 USC 103 as being obvious over Council and Hypponen et al. as applied to claim 1 and further in view of Hardy et al.

Applicants traverse these grounds of rejection.

As previously presented with respect to Ji et al., Hypponen et al. also fails to teach or fairly suggest forwarding or re-routing of e-mail messages received at a recipient computer to a screening server, such that the rejections in the Office Action mailed May 17, 2005 fail to make a *prima facie* case of obviousness.

While Hypponen et al. does not teach scanning at the recipient computer (as taught by Ji et al.), Hypponen et al. still ascribes to the prior art method of virus scanning by *interception* at a firewall/gateway *prior to ever being delivered to a recipient computer*. While Hypponen et al. suggests the re-routing of certain types of data to a screening server, it still relies on a few "protected systems" to intercept and re-route the mail, and thus the system will only work when a user is attached to the network with the "protected systems." In the present invention, the recipient computer can be connected to any network, not just a protected one.

Further, in the system of Hypponen et al., only certain types of data are intercepted and scanned; the agents on the protected systems must be updated to determine what is currently "suspect data." The present invention, however, re-routes *all* mail received by the recipient computer such that the only machine that needs up-to-date software is the screening server.

To address the prior art of record with respect to any teaching or suggestion of forwarding or re-routing of e-mail messages received at a recipient computer to a screening server, Applicants respectfully submit the following:

- Council - teaches screening of unwelcome or unsolicited email messages (which may contain a virus) based upon **delivering mail only if the sender is on an authorized list.**
- Hypponen et al. - discloses a method of detecting viruses in a computer network comprising **intercepting** data at at least one data **transit node** of the network. The transit nodes that employ the invention are called "protected systems" which are described in paragraph [0032] as "firewall **4***a*, mail server **4***b*, a proxy server **4***c* and a database server **4***d*." These protected systems are not **recipient computers** (called "users or clients **2**" in paragraph [0031]), but rather **transit computers**, and they identify which of the network data is of a type capable of containing a virus and transfers the identified data to a virus scanning server **7** over the network. In use, an email recipient is only protected when accessing email over the network that has the protected systems.
- Ji et al. - teaches virus scanning **at the client node** (recipient computer). See, e.g., the abstract and figures 11a-11c and the related text in columns 15-16.
- Hardy et al. - teaches **password-based authorization** and has no teachings regarding virus screening.
- Kim et al. - teaches virus scanning, sniffing, or detecting of e-mail viruses **prior to the e-mail messages arriving at the destination system** or server.
- Aronson et al. - teaches a server for filtering e-mail messages wherein the server receives requests to retrieve e-mail messages on behalf of a client and then retrieves e-mail messages from a mail server on behalf of the client. The **server then filters** the e-mail messages based on one or more rules and transfers the filtered e-mail messages to the client.
- Franczek et al. - teaches the screening of computer data for viruses within a telephone network **before communicating the computer data to an end user.**
- Tso et al. - teaches a system for virus checking a data object to be downloaded to a client device that is implemented in a method including the steps of retrieving a data object to be downloaded, scanning the data object for a computer virus, and **downloading the data object to the client device if no computer virus is detected.**
- Dickenson et al. - teaches an **e-mail firewall** that applies policies to e-mail messages between a first site and a plurality of second sites in accordance with a plurality of

administrator selectable policies.

- Chen et al. - teaches a message system, **located at the server computer**, that **controls the distribution of e-mail messages**, wherein an anti-virus module, located at the server computer, scans files for viruses.

None of these prior art systems include **recipient computer software** to re-route or forward received email to a scanning server. The prior art is primarily drawn to interception and scanning/cleaning of email at intermediate points in the delivery process. Hypponen et al. continues to teach this sort of system based upon interception by "protected systems" prior to suspect data being delivered to a user on the network with the protected systems.

Conclusion

For the reasons cited above, Applicants submit that claims 1-15 are in condition for allowance and requests reconsideration of the application. If there remain any issues that may be disposed of via a telephonic interview, the Examiner is kindly invited to contact the undersigned at the local exchange given below.

Respectfully submitted,

Christopher B. Kilner
Registration No. 45,381
Roberts Abokhair & Mardula, LLC
11800 Sunrise Valley Drive, Suite 1000
Reston, VA 20191-5302
(703) 391-2900